**AMENDMENTS TO THE SPECIFICATION:**

*Please amend the caption on page 1, line 6, as follows:*

~~BACKGROUND TO THE INVENTION~~RELATED ART AND OTHER CONSIDERATIONS

*Please amend the caption on page 3, line 27, as follows:*

BRIEF SUMMARY ~~OF THE PRESENT INVENTION~~

*Please amend the paragraphs beginning at page 3, line 28, and continuing to page 5, line 3, as follows:*

In accordance with a first aspect of ~~the present invention~~an example embodiment there is provided a method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes, the method comprising (a) generating a numerical chain comprising a series of values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; (b) sending a value from the first numerical chain from the mobile node to an access node to which the mobile node wishes to attach; and (c) using the sent value at the access node to authenticate the mobile node.

In accordance with a second aspect of ~~the present invention~~an example embodiment there is provided a method of deriving a secure authentication key when a mobile node authenticates itself to an access node in accordance with any preceding claim, the method comprising providing a first authentication key $K_{S0}$ for use by the mobile node and a first access node; sending a hash of the first authentication key hash($K_{S0}$) to a second access node and the mobile node; and generating a new authentication key $K_{S1}$ in accordance with the hash hash($K_{S0}$).

In accordance with a further aspect of ~~the present invention~~an example embodiment there is provided a mobile wireless terminal, the terminal comprising means for generating and storing a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for disclosing values from the numerical chain to an access node in order to allow the access node to authenticate the mobile wireless terminal.

In accordance with a further aspect of ~~the present invention~~an example embodiment there is provided an access node of a communication system having means for receiving from a mobile node a value of a first numerical chain comprising a series of n values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value; and means for authenticating the mobile node on the basis of that value.

*Please amend the paragraphs beginning at page 5, line 6, and continuing to page 5, line 9, as follows:*

FIG. 2 illustrates diagrammatically the architecture of a communications network in accordance with an example embodiment ~~of the present invention~~; and

FIG. 3 is a flow diagram illustrating the method of certain example embodiments ~~of the present invention~~.

*Please amend the paragraph beginning at page 5, line 11, and continuing through the remainder of page 5, as follows:*

FIG. 2 illustrates diagrammatically the architecture of a cellular communications network for mobile wireless terminals in accordance with a first example embodiment ~~of the present invention~~, with like numerals representing like elements to those shown in FIG. 1. Access nodes 4, 6 are interconnected by a network. The network may be a

cellular telecommunications network, e.g. a 3G network, WLAN, a combination of 3G and WLAN networks, or any other type of cellular network. A subscriber to a home network 3 owns a mobile wireless terminal 1 and seeks to access services such as voice calls, Internet access, or other data services from a visited (foreign) wireless network 2. Prior to granting the subscriber access to the services, the visited network requires authorisation from the subscriber's home network. In order for the subscriber to be authenticated, the visited network sends an authentication request to the home network, which checks the subscriber details in the HLR 10. This authentication process is defined in the MAP, RADIUS and DIAMETER (RFC 3588) protocols and, for wireless networks in particular, in the 802.1x, 802.11i and EAP (RFC 2298) protocols. Upon successful authentication, the visited network stores the subscriber's details in its Visitor Location Register (VLR) 11. The UE may then access the service available from the visited network via a first access node 4.

*Please amend the paragraph beginning at page 9, line 7, and continuing to page 9, line 12, as follows:*

According to a further example embodiment ~~of the present invention~~, each time the UE wishes to attach itself to a new access node, it discloses an H value further along in the sequence than the next one, e.g. if the UE disclosed $H_3$ to the last access node it attached itself to, then it may disclose $H_5$ (or any higher H value, up to $H_n$) rather than $H_4$. In this case the new access node must apply the hash() function to the disclosed value more than once in order to compare its output to the most recently distributed public H value.

*Please amend the paragraph beginning at page 9, line 20, and continuing to page 11, line 4, as follows:*

In accordance with a further example embodiment ~~of the present invention~~ multiple numerical chains are generated by the UE and the home network so that the UE may use them in parallel on multiple interfaces. The multiple chains are generated using different seed values and the same one-way coding function. Alternatively, the multiple chains may implement a different one-way coding function, subsequent communications bearing an indication of which coding function has been implemented on a given chain. This creates a fast "multi-homing" mechanism where only a single initial authentication is required even on a node with multiple interfaces. A different numerical chain must be used for each interface in order to avoid a replay attack.

In accordance with a further example embodiment ~~of the present invention~~, the numerical chains are bound to a specific MAC address on an access node interface by modifying the one-way coding function such that $H_{i-1}$=hash($H_i$, MAC address), rendering it impossible for a third party to claim that a given numerical chain is valid for another MAC address. Even if a third party obtains the UE's MAC address, any attempt to imitate the UE will necessarily be stamped with the third party's own MAC address, and the access nodes will be able to reject this service request as being fraudulent.

In accordance with further example embodiments ~~of the present invention~~, there is provided a method for deriving a secure authentication key for use when a UE switches access nodes as described above. It is initially assumed that the UE and the first access node share a common authentication key $K_{S0}$. Methods for achieving this are well-known. In a further embodiment, upon switching from a first access node to a new access node, the first access node sends a message containing the value hash($K_{S0}$) to the new access node, which sends these values to the UE. The UE can then confirm, by hashing $K_{S0}$ itself, that this message did indeed originate at the first access node. The UE and the new access node can then derive a new authentication key using the equation $K_{S1}$=hash(hash($K_{S0}$)). The new access node cannot determine the original authentication key $K_{S0}$ since it cannot reverse the one-way coding function hash($K_{S0}$) to obtain $K_{S0}$. The

message sent by the first node may also include a nonce $N_{P0}$, in which case the new authentication key is generated using the equation $K_{S1}$=hash(hash($K_{S0}$), $N_{P0}$).

In a further embodiment the first access node sends a hash of the authentication key, hash($K_{S0}$), to the new access node, and the mobile node and the new access node exchange nonces $N_{C1}$ and $N_{A1}$, a new authentication key being derived using the equation $K_{S1}$=hash(hash($K_{S0}$), $N_{C1}$, $N_{A1}$), such that the first access node cannot learn the new authentication key unless it intercepts the nonce exchange, and the new access node cannot learn the earlier authentication key since it cannot reverse the one-way coding function to obtain $K_{S0}$. In a still further embodiment, the first access node may also send a nonce $N_{P0}$ along with the value of hash($K_{S0}$), in which case the new authentication key is generated using the equation $K_{S1}$=hash(hash($K_{S0}$), $N_{P0}$, $N_{C1}$, $N_{A1}$).

The present ~~invention~~ technology provides a method of authenticating a mobile node to an access node of an access network. It will be appreciated by the skilled person that various modifications may be made to the above embodiments without departing from the scope of the present invention